SECURITY CHANGE NOTICE

Request email server info prior to firewall blocking
Info Required by October 31, 2004

Starting in early November, the Information Security Operations Center (ISOC) will start to block Port 25 (email service) at the Internet for unpermitted email servers within the State of Colorado network and MNT. Normal email through regular mail servers will not be impacted by this change. To avoid any possible interruption in service, we need you to send us your email server IP addresses so we can permit these prior to implementing this firewall block. Please fill out the attached form and return it to us by October 31, 2004.

You may permit as many addresses as you want as email servers. Please include application servers and network devices that send email alerts for service in this list. In the event that any email is blocked inadvertently, we will ensure that new permits are entered into the firewall in 48 hours or less. We will distribute a security variance form to be used for new and potentially missed servers by the end of the month.

Contact Info Also Requested

We are committed to working with you to make sure that we balance the need for a secure network with the need for a network that is available and reliable. To aid in that balance, we would like to develop better mechanisms for communicating security information to you so we are also asking you to provide a contact person for future changes or technical security information. We have also included email and phone numbers so you can contact us with your questions at the bottom of this memo.

Why We Are Making this Change

We are blocking this email service to computers that do not actively use it because studies of portions of our network have shown that almost 20% of all email and almost 50% of all spam contains malicious code. Some of this malicious code effectively turns the infected computer into a mail server that sends out more spam or malicious code- usually without any indication to the user. By blocking email traffic (Port 25) to and from unpermitted mail servers, we expect to stop a good deal of the infected mail. In addition, this action will force email through legitimate email servers that should be running active anti-virus scans. While this step alone will not eliminate malicious code or infected email on our network, it is an important first step. This action is also a recommended security best practice for Internet Access Providers by the Anti-Spam Technical Alliance (an standards industry group that includes Microsoft, Yahoo, America Online, British Telecom, Comcast, Earthlink, and other private and government organizations).

How to Contact Us with Questions
For questions about the attached form or policy change, please contact the DoIT Service Center at **303-239-4357 or 877-632-2487.**

You can also fax questions or concerns to us at **303-239-4609** or email us at:
ISOC@state.co.us

Thank you